UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,814	11/15/2001	Scott Fluhrer	50325-0596	3737

29989 7590 08/04/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/990,814	FLUHRER, SCOTT	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on 6/8/2005 with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

2. As per claim 1 and 17, Applicant remarks Cheng does not teach "description of network traffic that is to be protected". Examiner notes Applicant's arguments have been fully considered but are not persuasive. Cheng teaches the VPN security policy typically describes the characteristics of the protection for a particular traffic profile (Cheng: Column 6 Line 53 – 57: the traffic profile is interpreted as description of network traffic to meet the claim language). Furthermore, Cheng specifically teaches (a) the VPN security policy describes the protection of the flow of data between the plurality of nodes establishing the tunnel of the virtual private network (Cheng: Column 6 Line 55 – 57); (b) the endpoints of a particular tunnel are established by specifically defining the local ID (i.e. IP address), the local ID type (i.e. IPV4_address or IPV6_address) as well as remote ID (i.e. IP address) and remote ID type (i.e. IPV4_address or IPV6_address) (Cheng: Column 6 Line 11 – 15 and Figure 5 Element 530), which is qualified as the description of network traffic. Therefore, Cheng does teach the description of network traffic that is to be protected (Cheng: Column 6 Line 53 – 57, Column 6 Line 11 – 15 and Figure 5 Element 530).

3. Applicant further argues Cheng does not teach "creating and storing a third description of network traffic that is to be protected based on determining a logical

intersection of the first description of network traffic and the second description of network traffic". Examiner notes (a) Cheng teaches negotiating a common security policy (Cheng: Column 8 Line 53 – 55) so that data can be successfully transferred between the plurality of nodes establishing the tunnel (Cheng: Column 7 Line 29 – 30), (b) the security policy as taught by Cheng typically describes the characteristics of the protection for a particular traffic profile (Cheng: Column 6 Line 53 – 57, Column 6 Line 11 – 15 and Figure 5 Element 530: the traffic profile is interpreted as description of network traffic to meet the claim language), and thereby (c) the common security policy as taught by Cheng thus covers "a logical intersection of the first description of network traffic and the second description of network traffic" to meet the claim languages. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 5, 7, 11, 14 17, 18 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Cheng (Patent Number: 6823462), hereinafter referred to as Cheng.

As per claim 1, 14, 17, 18 and 20, Cheng teaches a method for determining secure endpoints of tunnels in a network that uses Internet security protocol (Cheng: see for example, Column 7 Line 21 – 15), the method comprising the computer-implemented steps of:

sending from a first network device a first description of network traffic that is to be protected; receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected (Cheng: see for example, Figure 4 & Column 7 Line 35 – 52 and Column 7 Line 23 – 25: entities to which network traffic may be directed are referred to as "hosts". Initiator as taught by Cheng is equivalent to the 1st network device associated with the source host and Responder is equivalent to the 2nd network device associated with the destination host);

creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic (Cheng: see for example, Column 7 Line 26 – 30: Cheng teaches establishing a tunnel having a tunnel definition by negotiating a common security policy associated with the client and the server); and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic (Cheng: see for example, Column 7 Line 26 – 30).

As per claim 5, Cheng teaches the claimed invention as described above (see claim 1). Cheng teaches the first description comprises a packet summary value that summarizes packets in the network traffic to be protected, and wherein the second description is generated by the second network device based on comparing the packet summary value to one or more access control lists that are managed by the second network device (Cheng: see for example, Figure 14 & Column 7 Line 46 – 57: security policy must fundamentally include access control rules).

As per claim 7, Cheng teaches the claimed invention as described above (see claim 1). Cheng further teaches determining, at the second network device, whether the packet summary matches a security policy information that is associated with the second network device; wherein the packet summary is associated with the first description of network traffic (Cheng: see for example, Column 7 Line 46 – 48).

As per claim 11, Cheng teaches the claimed invention as described above (see claim 1). Cheng further teaches receiving at the first network device an IP packet from a source end host that is associated with the first network device,; verifying that the IP

packet falls within the third description of network traffic (Cheng: see for example, Column 6 Line 58 – 60, Column 7 Line 21 – 30 and Column 7 Line 35 – 52).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2 – 4, 6, 8 – 10, 12 – 13 15 – 16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng (Patent Number: 6823462), hereinafter referred to as Cheng, in view of Bendinelli (Patent Number: 6631416), hereinafter referred to as Bendinelli.

As per claim 19, Cheng teaches an apparatus for determining secure endpoints of tunnels in a network that uses Internet security protocol (Cheng: see for example, Column 7 Line 21 – 15), comprising:

means for sending from a first network device a first description of network traffic that is to be protected; means for receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected (Cheng: see for example, Figure 4 & Column 7 Line 35 – 52 and Column 7 Line 23 –

25: entities to which network traffic may be directed are referred to as "hosts". Initiator as taught by Cheng is equivalent to the 1st network device associated with the source host and Responder is equivalent to the 2nd network device associated with the destination host).

However, Cheng does not disclose expressly the specific information described in the network traffic when exchanged between the 1st network device and 2nd network device includes port address, protocol type and proxy related information.

Bendinelli teaches the specific information described in the network traffic when exchanged between the 1st network device and 2nd network device includes port address, protocol type and proxy related information (Bendinelli: see for example, Figure 14 & Column 14 Line 18 – 32, Column 38 Line 30 – 45, Column 40 Line 27 – 42 and Column 45 Line 48 – 52).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bendinelli within the system of Cheng because Bendinelli teaches providing a method that can easily and effectively establish one or more virtual private networks over a local or wide geographical area to enable a secure tunnel (Bendinelli: see for example, Column 3 Line 50 – 60 and Column 14 Line 25 – 26).

means for creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic (Cheng: see for example, Column 8 Line 53 – 62); and

means for establishing the secure connection between the first network device and the second network device based on the third description of network traffic (Cheng: see for example, Column 7 Line 27 – 30).

As per claim 2 and 15, Cheng teaches the claimed invention as described above (see claim 1 and 14 respectively). Cheng does not disclose expressly the first description comprises a first set of proxies, wherein the second description comprises a second set of proxies.

Bendinelli teaches the first description comprises a first set of proxies, wherein the second description comprises a second set of proxies (Bendinelli: see for example, Figure 14 & Column 38 Line 30 – 46 and Column 14 Line 30 – 32).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bendinelli within the system of Cheng because Bendinelli teaches providing a method that can easily and effectively establish one or more virtual private networks over a local or wide geographical area to enable a secure tunnel (Bendinelli: see for example, Column 3 Line 50 – 60 and Column 14 Line 25 – 26).

Accordingly, Cheng in view of Bendinelli teaches the first description comprises a first set of proxies, wherein the second description comprises a second set of proxies, and wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of proxies and the second set of proxies.

As per claim 3 and 16, Cheng teaches the claimed invention as described above (see claim 1 and 14 respectively). Cheng does not disclose expressly the first description comprises a first protocol and the second description comprises a second protocol.

Bendinelli teaches the first description comprises a first protocol and the second description comprises a second protocol (Bendinelli: see for example, Figure 14 & Column 40 Line 28 – 37).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bendinelli within the system of Cheng because Bendinelli teaches providing a method that can easily and effectively establish one or more virtual private networks over a local or wide geographical area to enable a secure tunnel (Bendinelli: see for example, Column 3 Line 50 – 60 and Column 14 Line 25 – 26).

Accordingly, Cheng in view of Bendinelli teaches the first description comprises a first protocol and the second description comprises a second protocol, and further comprising the steps of determining a third protocol for the third description based on determining a logical intersection of the first protocol and the second protocol.

As per claim 4, claim 4 does not further teach over claim 3 because the result of a third protocol is based upon determining a logical intersection of the first protocol and

the second protocol. Therefore, see same rationale addressed above in rejecting claim 3.

As per claim 6, Cheng teaches the claimed invention as described above (see claim 1). Cheng further teaches the first description of network traffic comprises a packet summary includes IP protocol information that is associated with the network traffic emanating from a source end host, wherein the source end host is associated with the first network device; an IP address that is associated with the source end host; an IP address that is associated with the destination end host (Cheng: see for example, Column 7 Line 21 – 30, Column 6 Line 11 – 15 and Figure 5).

Cheng does not disclose expressly a packet summary that includes: port information that is associated with the source end host; port information that is associated with a destination end host, wherein the destination end host is associated with the second network device; and a proxy address of the source end host.

Bendinelli teaches a packet summary that includes: port information that is associated with the source end host; port information that is associated with a destination end host, wherein the destination end host is associated with the second network device; and a proxy address of the source end host (Bendinelli: see for example, Figure 14 / Figure 15A & Column 14 Line 18 – 32, Column 38 Line 30 – 45, Column 40 Line 27 – 42 and Column 45 Line 48 – 52).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bendinelli within the system of Cheng because Bendinelli teaches providing a method that can easily and effectively establish

one or more virtual private networks over a local or wide geographical area to enable a secure tunnel (Bendinelli: see for example, Column 3 Line 50 – 60 and Column 14 Line 25 – 26).

Cheng further teaches the second description is generated by the second network device based on comparing the packet summary to one or more access control lists that are managed by the second network device (Cheng: see for example, Column 7 Line 46 – 57).

As per claim 8, Cheng teaches the claimed invention as described above (see claim 1). Cheng further teaches the second description of network traffic comprises a response that includes: IP protocol information that is associated with the network traffic emanating from a destination end host, wherein the destination end host is associated with the second network device; an IP address that is associated with the second network device (Cheng: see for example, Column 7 Line 21 – 30, Column 6 Line 11 – 15 and Figure 5).

Cheng does not disclose expressly proxy addresses that are associated with a destination end host.

Bendinelli teaches proxy addresses that are associated with a destination end host (Bendinelli: see for example, Figure 15A & Column 38 Line 30 – 45). See the same rationale of combination applied herein as above in rejecting claim 2.

As per claim 9, Cheng in view of Bendinelli teaches the claimed invention as described above (see claim 8). Bendinelli further teaches the Proxy addresses that are associated with the destination end host include a first subnet that includes the destination end host and a second subnet that includes a source end host, wherein the source end host is associated with the first network device (Bendinelli: see for example, Column 45 Line 48 – 52 and Figure 15A).

As per claim 10, claim 10 encompasses the scope at least as described in claim 6 because the results of a third protocol information, port information and proxy information are based upon determining a logical intersection (i.e. common set as taught by Cheng) between the first and the second description of network traffic. Therefore, see same rationale addressed above in rejecting claim 6. Besides that, in further regards to claim 10, Bendinelli further teaches additional protocol information (Bendinelli: see for example, Column 40 Line 26 – 46).

As per claim 12, claim 12 is similar to claim 6 because the result of a third port information is based upon determining a logical intersection (i.e. common set as taught by Cheng) between the first and the second description of network traffic. Therefore, see same rationale addressed above in rejecting claim 6.

As per claim 13, claim 13 is similar to claim 6 because the claim imitation is an obvious outcome of the logical intersection as performed on the port information. Therefore, see same rationale addressed above in rejecting claim 6.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100